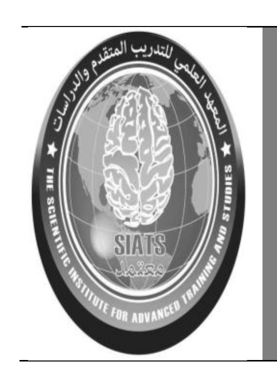


SIATS Journals

Journal of Human Development and Education for specialized Research

(JHDESR)

Journal home page: http://www.siats.co.uk



مجلة التنمية البشرية والتعليم للأبحاث التخصصية

العدد 4، المجلد 1 ، أكتوبر 2018م.

e ISSN 2462-1730

DEVELOPING MECHANISMS AND LEGAL SYSTEMS TO COMBAT CYBER-CRIME

تطوير الآليات والنظم القانونية لمكافحة الجرائم المعلوماتية

رؤية مستقبلية

د/زوزو هدى

مخبر أثر الاجتهاد القضائي على حركة التشريع

houhouhouda72@gmail.com

أ/ أحمد صابر

قسم الحقوق بكلية الحقوق والعلوم السياسية بجامعة محمد خيصر بسكرة الجزائر

2018م\1439هـ



ARTICLE INFO
Article history:
Received 1/9/2017
Received in revised form 20/9/2017
Accepted 11/12/2017
Available online 15/10/2018
Keywords:
Insert keywords for your paper

Abstract:

Informatics emerged as a product of scientific evolution and technical progress known in the world since the mid - twentieth century, and with time, nowadays, systems of electronic treatment of information dominate all aspects of daily and practical life of individuals, institutions and different companies, and even countries and various organizations. However, with all what these modern techniques possess of benefits, they produced a new pattern of crime; namely: **Cybercrime**.

All crimes that the world is witnessing nowadays and what it knew of destruction and disorder; especially in the Arab countries, like terrorist crimes, organized crimes, espionage, war crimes and different cross-border crimes are performed, today, using information systems. All of this makes us stand to think carefully and wisely to confront this modern way of criminality. Moving on a first step can not be made only through innovation and activation of new and ingenious methods to counter such crimes in line with the specificity characterized by it.

Therefore, this research study deals with a subject relating to develop and activate legal and innovative mechanisms to counter cybercrime, through changing research and inquiry methods about the cyber crimes, as well as the development of methods of international cooperation, and especially Arab cooperation, to create mechanisms in line with the requirements of this type of crimes. This can only be achieved by amending the internal legal systems of Arab countries by incorporating legal rules creating research and investigation systems and create a list based upon human and specialized technical structure, on the one hand; and the development of research ways by making them cross-bordering researches, on the second hand. This, by creating an internal Arab legislative cooperation channels without being faced with obstacles of sovereignty but the real wish to unify the legal patterns of legal and technical tracking. All of this to achieve real results for reducing crime



based on information as well as to facilitate pursuing of its perpetrators and to arrest them.

ملخص:

ظهرت المعلوماتية كنتاج للتطور العلمي والتقدم التقني الذي عرفه العالم منذ منتصف القرن العشرين، ومع الزمن أصبحت اليوم نظم المعالجة الإلكترونية للمعلومات تهيمن على كافة نواحي الحياة اليومية والعملية للأفراد والمؤسسات والشركات المتنوعة وحتى الدول والمنظمات المختلفة، لكن مع ما كان لهذه التقنيات الحديثة من فوائد إلا أنها أفرزت نمطا جديدا من الإجرام يسمى: **الجرائم المعلوماتية،** فكل الجرائم التي يشهدها العالم اليوم وما يعرفه من دمار واضطراب، وخاصة في الدول العربية كالجرائم الإرهابية والجرائم المنظمة والتجسس وجرائم الحرب ومختلف الجرائم العابرة للحدود تتم اليوم باستخدام نظم معلوماتية، كل هذا يجعلنا نقف لنفكر مليا وبحكمة لمواجهة هذا الطريق الحديث للإجرام، فالانتقال كخطوة أولى لن يكون إلا من خلال ابتكار وإعمال طرق جديدة ومبتكرة لمكافحة هذه الجرائم تتماشى والخصوصية التي تتميز بها.

وعليه فإن هذه الدراسة البحثية تتناول موضوعا يتعلق بتطوير وتفعيل آليات قانونية مستحدثة لمكافحة الجريمة المعلوماتية، من خلال تغيير طرق البحث والتحري حول الجرائم المعلوماتية، وكذا تطوير طرق التعاون الدولي وخاصة العربي، لخلق آليات تتماشى ومقتضيات هذا النوع من الجرائم، وهذا لا يمكن أن يتحقق إلا من خلال تعديل النظم القانونية الداخلية للدول العربية بإدخال قواعد قانونية تخلق أجهزة بحث وتحري وتحقيق قائمة على هيكل بشري وتقني متخصص هذا من جهة، وتطوير طرق البحث بجعلها عابرة للحدود من جهة ثانية، وهذا بخلق قنوات التعاون التشريعي الداخلي العربي دون أن تعترضها عوائق السيادة بل الرغبة الحقيقية لتوحيد أنماط التتبع القانوني التقني، كل هذا لتحقيق نتائج فعلية في الحد من الإجرام بالاعتماد على المعلوماتية وكذا تسهيل ملاحقة مرتكبيها والقبض عليهم.

مقدمة :



ظهرت المعلوماتية كنتاج للتطور العلمي والتقني الذي عرفته البشرية، حتى أصبحنا اليوم نعيش في عصر الرقمنة أين تتدخل الانترنت في كل مجالات الحياة اليومية وفي معظم المعاملات على اختلاف أنواعها لما توفره هذه التقنيات من سرعة وعبور لكل الحدود، في عالم افتراضي يحول العالم إلى قرية صغيرة لا تعرف المسافات الجغرافية.

على **الرغم** من كل هذه المزايا التي وفرتها *المعلوماتية* **إلا** أنها في الآن ذاته *فتحت الباب على* مصراعيه لتسهيل ارتكاب عدد هائل من الجرائم بكل سهولة ويسر وسرعة، وابتكار طرق جديدة لطمس معالم هذه الجرائم دون ترك أي أثر، هذه الطائفة الجديدة من الجرائم تسمى الجرائم المعلوماتية، كل هذا يدفعنا إلى الوقوف للتفكير مليا بحكمة وروية لإعادة النظر في النظم القانونية التي تقف عاجزة أمام هذا الإجرام الجديد ومضطرة في الآن ذاته لإعادة التفكير في صيغ وآليات ونظم قانونية جديدة تجاري التطور الحاصل في ميدان الإجرام المعلوماتي، لأن مواجهة هذه الظاهرة والحد منها هو أول الخطى الضرورية للوصول إلى عصر الحكمة، لأن هذا الأخير لا يتجسد إلا في مجتمع يقضى فيه على وحش مدمر يحرك كل أشكال الجريمة اسمه الجرائم المعلوماتية، على هذا الأساس نطرح الإشكالية التالية:

ماهي الطرق و الآليات القانونية التي يمكن أن تساهم في الحد من الجرائم المعلوماتية و تطريق مرتكبيها لتكريس الحكمة المعلوماتية ؟ سيتم الإجابة على هذه الإشكالية من خلال خطة

المبحث الأول: ماهية الجرائم المعلوماتية

نتناول من خلال هذا المبحث الإطار المفاهيمي لهذا النوع من الجرائم، عبر الوقوف على التعريف القانوني السليم للجريمة المعلوماتية و كذا إظهار تميز هذا النمط الإجرامي الحديث بالعديد من الميزات و



الخصائص التي تميزه عن باقي الجرائم الكلاسيكية، مما يستدعي إحاطتها بآليات خاصة تتماشى و هذه الخصوصية ، كما نتناول في هذا المبحث مختلف أشكال و أنواع الجرائم المعلوماتية من خلال مطلبين.

المطلب الأول: مفهوم الجرائم المعلوماتية

للإحاطة بمفهوم الجرائم المعلوماتية لابد من الوقوف على تعريفها وكذا تحديد خصائصها، و هذا ما سنوضحه في الفرعين المواليين، الفرع الأول نتناول فيه تعريف الجرائم المعلوماتية أما الفرع الثاني فندرس فيه خصائصها.

الفرع الأول : تعريف الجرائم المعلوماتية

قبل التطرق إلى تعريف هذا النوع من الجرائم نشير إلى أن هذه الجريمة تستخدم بعدة تسميات فالبعض يسميها الجرائم الإلكترونية في حين يسميها البعض الآخر الجرائم الماسة بنظم المعالجة الإلكترونية للمعلومات، كما يطلق عليها آخرون تسمية الجرائم السيبرانية أو الاحتيال المعلوماتي أو الغش المعلوماتي وغيرها من المسميات التي تشير إلى مسمى واحد، فالاتجاه الغالب يميل إلى تسميتها بالجرائم المعلوماتية ، أو جرائم الحاسب الآلي و الانترنت، إذن الجريمة المعلوماتية – و هي التسمية المعتمدة من جانبنا – هي عبارة عن مصطلح مركب : الجريمة و المعلوماتية، إذا عرفنا الجريمة : هي كل سلوك مهما كان شكله (فعل أو امتناع) و مهما كانت طريقة ارتكابه مجرم قانونا، و يحدد له المشرع عقوبة ضمن قانون العقوبات أو القوانين المكملة و المتممة له .



أما المعلوماتية فنجد لها عدة تعاريف مثلا ((مجموعة من الحقائق التي يعبر عنها بالكلمات أو الحروف أو الأشكال أو الرموز))[1] وقد استخدم مصطلح المعلوماتية لأول مرة من قبل A.I.MIKLAILOV مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفياتي وسمي بعلم المعلومات العلمية .[2]

هذا و يعرفها البعض بأنها :((علم التعامل العقلاني بواسطة آلات أوتوماتيكية مع المعلومات باعتبارها دعامة للمعارف الانسانية و عمادا للاتصالات في ميادين مختلفة و متنوعة))[3]

عند الجمع بين المركبين نحصل على مصطلح : الجريمة المعلوماتية ، وفي بحثنا عن تعريف منضبط لهذا المصطلح وجدنا عدة صعوبات، هذا لحداثة هذا النوع من الجرائم من جهة ، و قيامها على تقنية علمية و معلوماتية عالية الدقة و التعقيد، إضافة إلى تجنب التشريعات الجنائية المقارنة وضع تعريف لهذا النوع من الجرائم من جهة أخرى .

إذا نجد أن هناك تعاريف ركزت على وسيلة ارتكاب الجريم ، وأخرى ركزت على شخصية مرتكبها (المجرم المعلوماتي) في حين ربطته بعض التعريفات بتوافر التقنية المعلوماتية، كما أن هناك تعريفات متمحورة حول موضوع الجريمة في حد ذاتها، إضافة إلى وجود تعاريف مختلطة ومتنوعة .

هذا ونلاحظ أنه سواء ركز التعريف على الوسيلة أو الموضوع أو الشخص فإنه يندرج ضمن التعاريف الضيقة، وكلما كان التعريف أكثر اختلاطا وتنوعا كان تعريفا واسعا، ولهذا سنتناول في دراستنا لهذا الموضوع تقسيم الفقهاء إلى اتجاهين، اتجاه ضيق وآخر واسع .

---

[1] سامي علي حامد عياد ، **الجريمة المعلوماتية و إجرام الانترنت** ، دار الفكر الجامعية ، الاسكندرية ، 2007 ، ص 23 .
[2] نفس المرجع السابق، ص 35 .
[3] **تعريف للأكاديمية الفرنسية**، في الجلسة المنعقدة بتاريخ 1967/04/06 م ، ص 08 .



أولا : الاتجاه الضيق

من التعريفات الضيقة للجرائم المعلوماتية، نجد تعريف الفقيه **Merioe** بقوله: ((الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي .)) [4]

كما يرى البعض الآخر ومنهم الأستاذ **trédman** أن: ((الجريمة المعلوماتية هي تلك التي تشمل أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات))[5]

سواء نظرنا إلى التعريف الأول أو الثاني فإن كلاهما غير جامع و لا مانع، كون التعريف الأول يركز على وسيلة ارتكاب الجريمة المتمثلة في الكمبيوتر مهملا العالم الافتراضي والانترنت التي تشكل الميدان الخصب للإجرام الاكتروني، أما التعريف الثاني يركز على محل الجريمة الإلكترونية وهو المال، في حين أن المال لم يعد المحل الوحيد لهذا النوع من الجرائم، بل امتدت لتشمل الأشخاص من كل الفئات والأعمار كالجرائم الموجهة للأطفال والمراهقين بكل أشكالها، وكذاجرائم الشرف والعرض كجرائم التشهير والسب والقذف وغيرها

من التعارف الواردة في هذا الشأن نجد تعريفا لمنظمة التعاون الاقتصادي والتنمية الخاص باستبيان الغش المعلوماتي عام 1982 بقولها: ((كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية و المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية)) .[6]

كما يعرفها البعض بأنها: ((كل نشاط غير مشروع موجه للنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها)).[7]

---

[4]Merur vender **; computer crimes and other crimes** ; against information technologgy in south africa .R.I.D.P . . South Africa ; 1993 ; p 554 .
[5] K trédman.**fraude et autres délits d’affairaes commis à l’aide de l’ordinateures éléctroniques**.rev.de.pén.crim.Paris.1984.P612.
[6] نائلة عادلة محمد قورة ، **جرائم الحاسب الآلي الاقتصادية** ، دراسة نظرية و تطبيقية ، منشورات الحلبي الحقوقية ، 2005 ، ص 32 .
[7] محمود أحمد عبابنة ، **جرائم الحاسوب و أبعادها الدولية** ، دار الثقافة للنشر و التوزيع ، الأردن، 2005 ، ص 17.



نجد أن هذه التعريفات أيضا منتقدة وغير جامعة ولا مانعة كونها تركز على موضوع الجريمة أو محلها مهملة الجانب الشخصي والمعنوي والتقني في هذا النوع من الجرائم .

في هذا الإطار هناك من يرى أن الجرائم المعلوماتية هي : ((كل فعل اجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل)).[8]

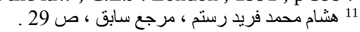
كما عرفها البعض أنها : ((ذلك النوع من الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها و مقاضاة فاعلها .)).[9]

هذه التعريفات أيضا قاصرة عن الإلمام بمختلف أوجه ظاهرة الاجرام المعلوماتي كونها ركزت على الفاعل أو المجني عليه أو الطريقة المتبعة لارتكابها الأمر الذي يجعلنا مضطرين للانتقال للاتجاه الثاني .

ثانيا : الاتجاه الواسع

مع تطور المعلوماتية والانتشار السريع لشبكة الانترنت وامتدادها بشكل واسع حول الكوكب إلى قرية صغيرة ظهرت أشكال جديدة للجرائم المعلوماتية، الأمر الذي جعل التعاريف الضيقة لا تتماشى وواقع الوتيرة السريعة والمتنوعة لهذا النوع من الجرائم، الأمر الذي دعى إلى ضرورة اعتماد تعاريف أكثر اتساعا لتشمل أكبر قدر ممكن لكل أوجه وأشكال الجرائم المعلوماتية .

من التعريفات الواسعة نجد مثلا : ((كل سلوك اجرامي يتم بمساعدة الكمبيوتر))[10] ، وكذا: ((كل تلاعب بالحاسوب الآلي و نظامه من أجل الحصول بطريقة غير مشروعة على مكسب أو إلحاق خسارة بالمجني عليه)). [11]



[8]B.D.Parker. **combattre la criminalité informatique** . édoro . paris . 1985 . p 18 .

[9] هشام محمد فريد رستم ،((الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني)) ، كلية الشريعة و القانون ، جامعة الإمارات المتحدة ، المجلد الثاني ، الطبعة الثالثة ، 2004 ، ص 407 .

[10] Adrian Roden **; Computer crimes and the law** ; C.L.J . London ; 1991 ; p 399 .

[11] هشام محمد فريد رستم ، مرجع سابق ، ص 29 .



نلاحظ أن هذه التعاريف رغم اتجاهها الموسع إلا أنه توسيع فيه مصادرة على المطلوب، كونها تجعل كل جريمة مهما كان نوعها ترتكب بواسطة جهاز الكمبيوتر من قبيل الجرائم الالكترونية وهذا غير صحيح، ذلك أن هناك عددا لابأس به من الجرائم الكلاسيكية التي ترتكب بواسطة جهاز الكمبيوتر كسرقة المعلومات باستخدام الوسائط أو تخريب الوحدة المركزية للجهاز أو أحد مكوناته .

من التعاريف المقترحة في هذا الإطار : ((جرائم المعلوماتية تعني جرائم الشبكة العالمية التي يستخدم الحاسوب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة)) . [12]

في تعريف آخر : ((هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها)) . [13]

رغم ما يوجه لهذه التعاريف من انتقادات كونها تعاريف وصفية ولا تعطي الماهية الحقيقية للجريمة المعلوماتية إلا أنها تبقى الأشمل لمعظم صور هذه الطائفة من الجرائم ودون التركيز على جانب دون الآخر، في محاولة لعدم إفلات أي من الفاعلين لأي نوع من أنواعها.

الفرع الثاني : خصائص الجرائم المعلوماتية

---

[12] يونس عرب ، **صور الجرائم المعلوماتية و اتجاهات تبويبها** ، ورقة عمل مقدمة لورشة تطوير التشريعات في مجال مكافحة الجرائم الالكترونية ، هيئة تنظيم الاتصالات ، هيئة تنظيم الاتصالات ، سلطنة عمان ، 2006 ، ص 06 .

[13] نفس المرجع السابق ، ص 07 .



من خلال التعاريف السابقة نلاحظ أن هذا النوع من الجرائم له مجموعة من الخصائص والمميزات التي تميزها عن غيرها من الجرائم، هذه الخصائص جعلت منها ظاهرة إجرامية خطيرة وممتدة تحتاج إلى آليات ونظم قانونية خاصة للوقاية منها ومكافحتها، من جملة هذه الخصائص نجد مايلي :

أولا : الجرائم المعلوماتية جرائم ترتكب بواسطة أجهزة الإعلام الآلي وعبر شبكة الانترنت

حتى نكون أمام جريمة معلوماتية لابد من أن تكون مرتكبة في العالم الافتراضي عبر شبكة الانترنت، وهذا لا يتحقق إلا بواسطة جهاز من أجهزة الإعلام الآلي، قد يكون الحاسوب الآلي أو المحمول ومختلف الأجهزة الذكية كالسمار ت فون أو الآيباد و غيرها .

ثانيا : هي جرائم عابرة لحدود الدول

إن العالم المعلوماتي الافتراضي لا يعرف حدودا جغرافية، بل يشكل مجتمعا مفتوحا عبر شبكات غير مرئية تخترق الزمان والمكان، الأمر الذي جعل مسرح الجريمة يتسم بالعالمية لا المحلية مما يضفي على هذا النوع من الجرائم الصبغة الدولية لعبورها حدود الدول.

هذا الأمر أفرز مشاكل لا حصر لها منها صعوبة تحديد الدولة صاحبة الاختصاص القضائي للجريمة و كذا القانون الواجب التطبيق هل الدولة التي يوجد بها الفاعل أم الدولة التي حدث فيها الضرر. ونظرا لعدم تواجد الجاني والمجني عليه



على نفس مسرح الجريمة، بل يرتكب الفاعل الجريمة عن بعد إذن لا تقف الجريمة المعلوماتية عند حدود مما يؤدي إلى صعوبة اكتشافها وصعوبة ملاحقة واكتشاف مرتكبيها، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الكمبيوتر الموجود في بلد آخر، وهو بهذا السلوك قد يضرر بأشخاص موجودين في بلدان أخرى، أو القيام بإعداد برنامج خبيث (Virus) في بلد ما ثم ينسخ ويرسل إلى مختلف دول العالم ، و يظهر هذا الاشكال بصفة خاصة في التعاملات البنكية عبر شبكات المعلومات الدولية وفي ميدان التجارة الإلكترونية، و هذا يطرح إشكالا آخر هو الاصطدام مع سيادة الدول وقوانينها العقابية المتعارضة الأمر الذي يقف حائلا دون إمكانية ملاحقة المجرمين أو حتى وصول القضايا إلى دور القضاء.

ثالثا : صعوبة اكتشاف الجرائم المعلوماتية وإثباتها

تتميز الجرائم المعلوماتية بصعوبة اكتشافها، هذا لكونها تحدث في عالم افتراضي فلا عنف ولاسفك دماء و لا كسر أو خلع، وإنما أرقام و بيانات تمحى أو تتغير أو ترسل إلكترونيا، إذن هي جرائم لا تخلف آثارا ورائها يمكن أن نتبعها كما هو الحال في الجرائم الكلاسيكية، كما أنها ترتكب من أشخاص على علم ودراية بالمعلوماتية الأمر الذي يجعلهم قادرين على تدمير أي دليل يمكن أن يكشفهم أو يدل عليهم في وقت قياسي.

كما أن المجني عليه يلعب دورا رئيسيا في عدم إمكانية اكتشافها إذ نادرا ما يقوم بالابلاغ عنها لأسباب قد تتعلق بسمعة المؤسسة أو الشركة مخافة زعزعة الثقة بها وبالتالي تراجع نسب التعامل معها. [14]

كل هذا ينتج عنه صعوبة اكتشافها لكونها قائمة على وسائل تقنية عالية الدقة، الأمر الذي يجعل المحقق التقليدي لا يمكنه الاعتماد على وسائل الاثبات العادية والأدلة التقليدية التي لا تتلائم مع طبيعة هذه الجرائم الناعمة والخفية،

---

[14] هشام فريد رستم ، مرجع سابق ، ص 41.



فلا شهود عاينوا الواقعة ولا عنف ولا ضوضاء الأمر الذي ينجر معه أنه حتى في حالات الإبلاغ عن هذه الجرائم أو اكتشافها يصعب اثباتها، الأمر الذي ينتج معه إفلات الجناة من العقاب.

رابعا : خصوصية المجرم المعلوماتي وأساليب ارتكاب الجرائم المعلوماتية

تتميز هذه الجرائم بسمات خاصة في مرتكبيها، كونها جرائم تقنية كما أن الأشخاص القائمين بها عادة يكونون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل ممن لديهم حد أدنى من المعرفة والدراية و القدرة على استعمال الكمبيوتر وشبكة الانترنت، مثلا جرائم التحويل المالي الإلكتروني غير المشروع للأموال يتطلب مهارة قدرة فنية وتقنية عالية جدا من قبل مرتكبيها.[15]

لكن هذا لا يعني بالضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم والدراسة، بل إن الواقع العملي أثبتت أن أنجح الجرائم من مجرمين لم يتلقوا المهارة اللازمة عن طريق التعليم أو الخبرة من العمل في المجال، بل قد يكونون مراهقين أو حتى أطفال ولكن لديهم قدرات عالية في التحكم في أسرار وعالم الانترنت.

المطلب الثاني: أنواع الجرائم المعلوماتية

ينطوي تحت تسمية الجرائم المعلوماتية طوائف وأنواع عديدة من الجرائم المتنوعة، وهي إما أن تكون جرائم موجهة ضد النظام المعلوماتي في حد ذاته أو أنها جرائم تستخدم النظم المعلوماتية للوصول إلى غايات وأهداف إجرامية، إذ نجد تحت كل نوع أعدادا لا حصر لها من الجرائم، وهذا ما سنتناوله فيما يلي:

الفرع الأول : الجرائم على النظم المعلوماتية

---

[15] المرزوقي محمد محمود ، **((الجرائم الحاسب الآلي))** ، المجلة العربية للفقه و القضاء ، صادرة عن الأمانة العامة لجامعة الدول العربية، العدد 28 ، 2003 ، ص63.



تتمثل في تلك الجرائم التي يكون فيها النظام المعلوماتي هو الهدف من النشاط الإجرامي و نجد عدة أنواع منها:

أولا : سرقة وتحويل المال المعلوماتي

هنا يكون المال المعلوماتي هو موضوع الجريمة سواء بالاعتداء على المال بسرقته أو النصب و خيانة الأمانة أو التحويلات المالية غير المشروعة.

ثانيا : الدخول إلى المواقع المحجوبة (استخدام البروكسي)

البروكسي هو برنامج يستخدم لتجاوز المواقع المحجوبة وعادة ما تكون مواقع جنسية أو معادية للدولة، وقد يتم حجب بعض المواقع التي لا يفترض حجبها كالمواقع العملية أو تلك التي تنشر إحصائيات عن الجرائم.[16]

ثالثا: جرائم الاختراقات

يعد الهجوم على المواقع واختراقها أو اقتحامها والتسلل إليها من الجرائم الشائعة في العالم ويشمل تدمير الموقع، اختراق مواقع رسمية أو شخصية، اختراق الأجهزة الشخصية والتحكم بها، اختراق البريد الإلكتروني للآخرين أو إغراقه بالرسائل، أو الاستلاء على اشتراكات الآخرين وأرقامهم السرية وإرسال الفيروسات.[17]

رابعا : جرائم التزوير

[16] سامي علي حامد عياد ، مرجع سابق ، ص 79 .

[17] رصاع فتيحة ، ((**الحماية الجنائية للمعلومات على شبكة الانترنت**)) ، مذكرة مقدمة لنيل شهادة الماجستير في القانون العام ، جامعة تلمسان ، الجزائر ، 2011 /2012 ، ص 75 .



هي من أكثر الجرائم رواجا فلا تكاد تخلو جريمة معلوماتية من شكل من أشكال التزوير، من خلال الدخول إلى قاعدة البيانات وتغييرها إما بإضافة معلومات مغلوطةأو محو معلومات ووضع أخرى غير صحيحة للحصول على أرباح غير مشروعة. [18]

خامسا : جرائم قرصنة البرامج والبرامج المعادية

جرائم القرصنة وتعني النسخ غير المشروع لنظم التشغيل أو البرامج الآلية، وحتى سرقة وتوزيع هذه البرامج دون إذن المالك أو دون ترخيص، متى كانت المادة تتمتع بحقوق النشر والتأليف فمثلا : ادعت الشركة APPLE ضد شركتي hewelt packard و Microsoft تتهمهما بالاستيلاء على بعض البنود من برامجها بنسخها دون إذن المالك. [19]

أما البرامج المعادية فقد تكون معادية للأشخاص أو للهيئات كالمواقع السياسية المعادية للدولة أو المعادية لدين معين أو لشخص معين تهدف إلى تشويه سمعته.

الفرع الثاني : الجرائم باستخدام النظم المعلوماتية

هي تلك الطائفة من الجرائم التي تستخدم الانترنت وسيلة لارتكاب جرائمها، وهي كثيرة ومتنوعة من أمثلتها:

أولا : الجرائم الجنسية والممارسات غير الأخلاقية

---

[18] سامي علي حماد ، مرجع سابق ، ص 81

[19] اللبان شريف ، **تكنولوجيات الاتصالات : المخاطر و التحديات و التأثيرات الاجتماعية** ، الدار المصرية اللبنانية ، القاهرة ، 2000 ، ص114 .



من أخطر ما أفرزته المعلوماتية والانترنت وجود مواقع مشبوهة تدعو إلى إقامة علاقات غير شرعية، بقصد جني الأرباح لتسويق الفتيات والسيدات والمتاجرة بالقصر والأولاد ومن أشهر هذه المواقع نجد مثلا : الموقع الأمريكي المسمى ((العزاب الأمريكيون)) أو Americansingles.com [20]

ثانيا : الجرائم الواقعة على الحياة الخاصة و إفشاء الأسرار

تكون بالتشهير بالأشخاص أو بجماعات معينة من خلال نشر معلومات تتعلق بحياتهم الخاصة، وهي تسبب أضرارا مادية ومعنوية من خلال القذف أو السب أو تشويه السمعة حتى ولو كانت معلومات صحيحة وليست بالضرورة غير ذلك. إضافة إلى جرائم إفشاء أسرار الأشخاص أو الهيئات أو الدول والمنظمات، كل هذا لإلحاق أضرار معتبرة بهم و تحقيق ربح للجاني.

ثالثا : الجرائم المالية

نجدها كثيرة ومتنوعة منها السطور على أرقام بطاقات الائتمان وكذا القمار على الانترنت بالالتفاف حول صفحة الأنترنت و كل مقامر في منزله، إضافة إلى مختلف جرائم التجارة الالكترونية.

رابعا : الجرائم المنظمة

استغلت العصابات ومافيا الجريمة المنظمة ما توفره الامكانات المتاحة عبر الانترنت من توسيع نشاطها وكذا تطوير أساليب التخطيط والتنفيذ والتوجيه للعمليات الإجرامية في يسر وسهولة، بسبب سهولة النقل السريع للمعلومة ونشرها في لمح البصر، من أمثلتها الجرائم الإرهابية وغسيل الأموال والاتجار بالمخدرات وغيرها....

---

[20] سليم طارق عبد الوهاب ، ((**الجرائم المرتكبة بواسطة الانترنت و سبل مكافحتها**)) ، بحث مقدم إلى الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة ، لمجلس وزراء الداخلية العرب ، تونس ، 07-09-1997 م .



لنصل إلى القول أن هذه الطوائف والأنواع كثيرة ومتنوعة ومتطورة ومتجددة بتطور وتجدد عالم الانترنت والتكنولوجيا الأمر الذي يجعلها تأبى الحصر والتحديد، بل هذا يستدعي نظما وآليات جديدة لمحاولة الوقاية من هذه الجرائم، وفي حالة وقوعها بتطويقها ووقفها قدر الإمكان، كون هذا الأخير مطلب هام وأساسي للوصول إلى عصر المحكمة والتنمية خاصة في الدول العربية ، و هذا ما سنتناول تفصيله في المبحث الموالي :

المبحث الثاني: أليات مكافحة الجريمة المرتكبة عبر الإنترنت

إن التنامي الهائل والخطير لشتى أنواع الجرائم المعلوماتية فرض حتمية الحكمة التشريعية لمواجهة هذا النوع من الإجرام الذي يتصادم مع تخلف النصوص القانونية وخاصة العربية منها في إطار ضآلة التعاون الإقليمي الفعال لمواجهة هذا الخطر، كل هذا يدعوا إلى ضرورة البحث عن آليات و قنوات مستحدثة وفعالة للحد من هذه الظاهرة التي تشكل حجر عثرة في طريق الولوج إلى عصر الحكمة خاصة على المستوى العربي، وعليه سنتناول من خلال المطلبين المواليين مجموع الآليات القانونية التي نرى أنها ضرورية لمكافحة الإجرام المعلوماتي، من خلال تطوير وتعديل القوانين الداخلية، مع ضرورة إرساء تعاون دولي عربي حقيقي على غرار التعاون الغربي مثلا من خلال إتفاقية بودابست التي ارست قواعد إجرائية حقيقية لمواجهة هذا الخطر، و هذا لا نجده على المستوى العربي.

المطلب الأول:تطوير النظم القانونية الداخلية

إن الناظر إلى طرق مواجهة الجرائم المعلوماتية في التشريعات المقارنة يمكن أن يميز بين اتجاهين رئيسيين هما:

إتجاه استحدث قوانين خاصة تتعلق بمكافحة هذا النوع من الجرائم ومن أمثلتها: الجزائر التي أصدرت القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[21].وكذا المشرع

(21) القانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق ل05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها.



الأردني بإصداره قانون جرائم أنظمة المعلومات [22]وكذا القانون السوداني سنة 2006 ، وقانون الإمارات المتحدة رقم 02 الصادر في 2006 في شأن مكافحة جرائم تقنية المعلومات، وقانون المملكة العربية السعودية بالمرسوم الملكي رقم 17 بتاريخ 1428/03/08، وفي فرنسا صدر القانون رقم (19) لسنة 1988 المتعلق بجرائم المعلوماتية المعدل سنة 1992 وعام 2000، وكذا في الولايات المتحدة بالقانون الصادر في 08 فبراير 1996 م المعدل عام 1997، والمملكة المتحدة بالقانون الصادر عام 1990 م المسمى بقانون إساءة استخدام الحاسب الآلي، وكذا القانون السوداني لسنة 2006. [23]

إضافة إلى إتجاه ثاني إرتأى بإدخال تعديلات تسد الفراغ والنقص التشريعي ضمن نصوص قانون العقوبات تتعلق بمكافحة الجرائم المعلوماتية، كما فعل المشرع الجزائري بموجب القانون الصادر سنة 2006 الذي استحدث بموجبه الجرائم الماسة بنظم المعالجة الآلية للمعلومات الذي عدل قانون الإجراءات الجزائية الجزائري قبل إصدار القانون رقم 09-04، وكذا المشرع الألماني بالقانون الصادر في 15 ماي 1986 المعدل لقانون الإجراءات الجزائية الألماني، و المرسوم السلطاني العماني رقم 2001/72 الذي عدل أحكام قانون الجزاء العماني رقم 07 لعام 1974 بإضافة فصل تحت عنوان جرائم الحاسب الآلي. [24]

سواء كان التشريع ضمن الإتجاه الأول أو الاتجاه الثاني ففي جميع الأحوال هناك مجموعة من الصعوبات التي لا تزال عائقا أمام أحكام السيطرة على هذا النوع من الجرائم، وعليه سنتناول في الفرعين المواليين الصعوبات والعوائق التي

(22) قانون جرائم أنظمة المعلومات مؤقت رقم(30) لعام 2010.

(23) الرواشلات سامي و الهياجنة أحمد، مكافحة الجريمة المعلوماتية كالتجريم و العقاب، المجلة الأردنية في القانون و العلوم السياسية، جامعة مؤتة، الأردن، المجلد الأول، العدد الثالث،2009، ص ص 132، 133.

[24] المواد 276 مكرر و مرر 01 و 02و 03 و 04 في المرسوم السلطاني رقم 2001/72 المنشور بالجريدة الرسمية العمانية رقم 698 بتاريخ 2001/07/01 المعدل لقانون الجزاء العماني الفصل الثاني مكرر مضاف للباب السابع بعنوان جرائم الحاسب الآلي .



لازالت التشريعات المقارنة العربية تعاني منها، ونتناول في الفرع الثاني الحلول و المقترحات التي نرى أنها تمثل حلولا لمواجهة هذه الجرائم.

الفرع الأول: الصعوبات و المشاكل العملية التي تثيرها الجرائم المعلوماتية

من أهم المشاكل التي تواجه جهات البحث والتحري عن الجرائم والتحقيق فيها إعتماد الجرائم المعلوماتية على تقنيات علمية إجرامية عالية، فالتكوين العام للضباط وأعوان الشرطة القضائية وحتى القضاة لا تتماشى والتكوين العام العادي لهؤلاء، كل هذا يؤدي إلى قصور في استيعاب الأفعال الإجرامية من جهة، و إفلات الفاعلين وضياع الأدلة من جهة ثانية، وما يزيد من صعوبة الأمر أن الجناة في هذه الجرائم لهم مفرداتهم الخاصة ولغاتهم المتميزة وبرامجهم المعقدة التي تحتاج إلى درجة عالية من الخبرة في هذا المجال.

من الصعوبات التي تكتنف هذا النمط الإجرامي غياب الدليل المرئي، ذلك أن الأدلة التقليدية كالسلاح أو الأداة المستعملة في إرتكاب الجريمة يضبط ويمكن إدراكه من قبل رجال التحقيق [25] لكن مختلف الأدلة الرقمية تكون ضمن عالم إفتراضي لا وجود لإدراك حسي لها، بل تعتمد على التشفير والرموز والأكواد السرية والنبضات والأرقام والتخزين الإلكتروني، كل هذا يجعلها جرائم لا تخلف أثارا مرئية تكشف عنها، وهذا يسهل ويسرع إخفاءها وطمس معالم الجرائم الإلكترونية.

وعليه يسهل إخفاء الأدلة و تدميرها، في حين أن الإثبات الجنائي قائم على وجود أدلة تعيد رسم معالم الجريمة أمام القضاء، الأمر الذي يجعل عددا هائلا من الجرائم لا يصل أصلا إلى القضاء لسرعة التخلص من الدليل.

---

(25) عبد الفتاح بيومي حجازي، **الدليل الجنائي و التزوير في جرائم الكمبيوتر و الإنترنت**، بهجات للطباعة و التجليد، مصر، 2009، ص36.



هذا و يعرف الجناة في الغالب بالذكاء والتخطيط العميق والمسبق، الأمر الذي يجعلهم يحيطون أنفسهم بتدابير أمنية واقية تحول دون إمكانية تحديد أماكنهم أو هويتهم لإعاقة الرقابة على البيانات المخزنة أو المنقولة عبر حدود الدولة، وهذا يحد من قدرات جهات التحري و التحقيق على قراءتها، الأمر الذي يجعل صون حرمة البيانات الشخصية المخزنة في مراكز الحاسبات والشبكات المتعلقة بالأسرار التجارية العادية والإلكترونية أو بتدابير الأمن والدفاع أمرا بالغ الصعوبة. [26]

إضافة إلى الطابع العابر للحدود الإقليمية وما يثيره من مشاكل عملية إذا يقوم المجرمون بتطوير آليات معقدة لغسيل الأموال، والتجارة غير المشروعة (تجارة المخدرات، الرقيق، الدعارة، القمار...) والأنشطة الإرهابية والجرائم المنظمة بالإعتماد على ما تقدمه الشبكة العنكبوتية من آليات معقدة ، كل هذا يصعب تتبع العمليات من الناحية العلمية و الفنية أمام العوائق القانونية المتمثلة في: الإصطدام بمبدأ السيادة عند عبور الجرائم للحدود الوطنية، تعقيد إجراءات تسليم المجرمين والمساعدات القضائية الدولية، إضافة إلى مشكلة تنازع الإختصاص القضائي الدولي الإيجابي والسلبي، فقد يتم تسجيل الإبلاغ عن الجريمة في مكان ما من دولة ما، في حين أن الأدلة الجنائية توجد في دولة أخرى، والخسائر حدثت في دول أخرى، فكيف يعقد الإختصاص القضائي؟

الفرع الثاني: الحلول و المقترحات لتعديل التشريعات الداخلية للدول العربية

عندما نلقي نظرة على التشريعات الغربية وخاصة الأوروبية منها، نجد أنها خطت خطوات جادة نحو تعزيز التعاون الأوروبي لتسهيل إجراءات ملاحقة المجرمين ومكافحة الجرائم المعلوماتية من خلال عدة إتفاقية و محاولات أبرزها إتفاقية بودابست[27]، والتي تهدف غلى حماية المجتمع من جرائم الفضاء المعلوماتي لإرساء سياسة جنائية مشتركة، وهي إتفاقية

(26) هشام فريد رستم، مرجع سابق، ص427.

(27) اتفاية بودابست لمكافحة الجرائم المعلوماتية، 2001/11/23، تبناها رؤساء الدول و الحكومات الأعضاء في المجلس الأروبي.



تنظم لأول مرة قائمة لجرائم الكمبيوتر وأنماطها وطوائفها، وكذا إرساء تدابير موضوعية وإجرائية وتوجيهات عريضة تتطلب تحديدا منظبطا من المؤسسات التشريعية لدى وضعها القوانين الداخلية، مؤكدة على خصوصية الإثبات بالنسبة للجرائم المعلوماتية لهذا قدمت حلولا لتحقيق الإنسجام الإجرائي وقواعد تسهل وتسرع عمليات الإنابات القضائية ومسائل الضبط والتفتيش خارج حدود الدول.

أما فيما يخص التشريعات العربية فلا بد أولا من إصدار قوانين خاصة بالجرائم المعلوماتية تتنظمها بشكل تفصيلي بالنسبة للدول التي اكتفت باجراء تعديلات على قوانينها الاجرائية .

هذا و ينبغي على الدول العربية أن تكرس مختلف التدابير التشريعية والتقنية الكفيلة بحماية أنظمتها المعلوماتية السرية من خلال حماية نظم وبرامج التشغيل والتحويل الالكتروني للبنوك وكذا المعلومات الأمنية والعسكرية والسياسية مع تطويرها وتحديثها بشكل متجدد هذا من الناحية التقنية، أما من الناحية القانونية فلا بد أن تتضمن القوانين الاجرائية العربية أجهزة بحث وتحري وتحقيق متخصصة في ميدان الجرائم المعلوماتية تتلقى تكوينا متخصصا يراعى فيه أن تكون البرامج التكوينية على يد خبراء ومتخصصين على درجة عالية من الكفاءة، وذلك أن التكوين العادي والكلاسيكي لا يفي بالغرض، كما فعل المشرع الجزائري مثلا في القانون رقم 04/09 باستحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته ومن مهامها مساعدة السلطات القضائية الشرطة بشأن المعلوماتية.

ضرورة تطوير طرق البحث والتحري وأساليب جمع الأدلة كالتفتيش والمعاينة والاعتراض بتطويرها وجعلها تتماشى والطبيعة الإكترونية إضافة إلى تسريع الاجراءات و مد الاختصاص الإقليمي لمواكبة سرعة الجرائم المعلوماتية، وكذا الاعتماد على وسائل الإثبات الرقمي والإلكتروني لأن الإبقاء على الأدلة الكلاسيكية سيؤدي إلى إفلات آلاف الجرائم من العقاب، ذلك أن المبدأ السائد في الإثبات الجنائي هو مبدأ مشروعية الدليل الجنائي: أي لابد و أن يتماشى الدليل



مع الشروط الشكلية والموضوعية المنصوص عليها قانونا حتى يقبل لإثبات الجرائم، وعليه فإن الأدلة الرقمية لن تقبل قضائيا إذا لم يكن المشرع قد سمح مسبقا بالإعتماد عليها. من ثم لابد من إدخال تعديلات على القوانين الإجرائية تسمح بالإعتماد على الأدلة الرقمية لتطوير مهارات التحقيق وكذا إعتماد هيئات وجهات قانونية مصدرة لشهادات التوثيق الرقمي لتأكيد الهوية نظرا لأهميتها في التعاملات المصرفية وأعمال التجارة الإلكترونية والخدمات الحكومية الإلكترونية، وكذا إنشاء وكالات خاصة بالأمن المعلوماتي لتأمين المواقع الحكومية والخاصة وتأمين المعطيات.

ضرورة تشديد العقوبات الجزائية المقررة لهذه الجرائم حتى تكون رادعة وعدم إخضاعها للتقادم حتى لا يشكل ثغرة لإفلات الجناة.

ينبغي على الدول العربية أن تتبع سياسة جنائية مشتركة تهدف إلى خلق سياسات منسجمة لتسهيل ملاحقة الجناة، وخلق شبكات معلوماتية مشركة لتخزين ونقل الأدلة المتعلقة بالجرائم المعلوماتية من خلال تفعيل أطر التعاون الدولي، هذا ما سنتناوله في المطلب الموالي.

المطلب الثاني: تطوير طرق التعاون الدولي لمكافحة الجريمة الالكترونية

أمام تنامي و انتشار الوحش المعلوماتي، وعبوره لكل الحدود وعدم كفاية التدابير والتشريعات الداخلية للدول في مكافحة الجرائم المعلوماتية، كان لزاما على الدول أن تتعاون مع بعضها لإيجاد قنوات وآليات قانونية كفيلة بتوحيد وتنسيق الجهود لمواجهة هذا الخطر، في الحقيقة هناك جهود ومحاولات دولية وإقليمية وعليه سنتناول في هذا الإطار جهود منظمة الأمم المتحدة والانتربول وكذا جهود المجلس الأوروبي والدول العربية من خلال الفروع التالية :

الفرع الأول : جهود الأمم المتحدة و الانتربول



حظيت الجرائم المعلوماتية باهتمام على مستوى مؤتمرات الأمم المتحدة و من أبرزها :

المؤتمر الثاني عشر من 12 إلى 19 أفريل 2010 بالبرازيل تحت عنوان((استراتيجيت شاملة لتحديات عالمية)) و قد دعى إلى عقد اجتماع الفريق من الخبراء لدراسة شاملة لمشكلة الجريمة المعلوماتية و تدابير التصدي لها .[28]

المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية من 12 إلى أفريل 2015 بدولة قطر، وكان الموضوع الرئيسي للمؤتمر "إدماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع للتصدي للتحديات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي ومشاركة الجمهور" وقررت الجمعية العامة في قرارها رقم 184/67 مايلي : ((إنشاء حلقات عمل من بينها تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة ومنها جرائم المعلوماتية)). [29]

إضافة إلى العديد من القرارات والتوصيات للأمم المتحدة ، و لكنها في مجملها لا تعدو أن تكون توصيات و دعاوى للدول للتعاون في هذا المجال دون وضع أطر إجرائية فعالة .

أما عن المنظمة الدولية للشرطة الجنائية الأنتربول فهي منظمة تهدف إلى تعاون أجهزة الشرطة للدول الأعضاء على نحو فعال في مكافحة الجريمة، عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول الأعضاء، وذلك لضبط المجرمين بمساعدة أجهزة الشرطة للدول الأعضاء، ومدها بالمعلومات حول الجرائم المتشعبة في عدة دول، و منها جرائم الأنترنت .[30]

الفرع الثاني :الجهود الإقليمية

---

[28] نفس المرجع السابق .
[29] حكومة قطر الالكترونية ، صفحة المؤتمر :
http//www.moi.gov.qa/UNCCPCJDOha/Arabic /previous – Congrsses . html
[30] أمير فرج يوسف ، **الجرائم المعلوماتية على شبكة الانترنت** ، دار المطبوعات الجامعية ، مصر ، 2009 ، ص 36 .



إضافة إلى جهود هيئة الأمم المتحدة نجد عدة مبادرات أبرزها دور المجلس الأوروبي في محاولة منه للحد من الجرائم المعلوماتية، كان أبرزها الإشراف على اتفاقية بودابست الموقعة من قبل أعضاء المجلس بتاريخ 2001/11/23 إذ قامت 26 دولة أوروبية بالتوقيع عليها وشاركت أربع دول غير أوروبية فيها هي: اليابان، جنوب إفريقيا، الولايات المتحدة الأمريكية إذ استغرقت 4 أعوام لصياغتها نهائيا . [31]

إذ سبق وأشرنا أنها وضعت آليات إجرائية فعالة في إطار مكافحة الإجرام المعلوماتي، كما أنشأ المجلس الأوروبي في لوكسومبورغ عام 1991 شرطة أوروبية تكون همزة وصل بين أجهزة الشرطة الأروبية الملاحقة الجناة . [32]

إذن كل هذه الجهود الدولية الرامية إلى مواجهة هذه الجرائم لأن الدول بمفردها لا يمكنها مواجهتها، فالتعاون القضائي الدولي هو السبيل الوحيد لمكافحة هذه الجرائم لأنها عابرة للحدود ولابد من تبادل المساعدات القضائية والخبرات المعلوماتية لأن مبدأ السيادة يقف عقبة أمام تسليم الرعايا، ذلك أن المساعدة القضائية تكون من خلال التعاون القضائي الدولي بتبادل المعلومات وإمكاية نقل الإجراءات في إطار المشروعية المكرسة بمعاهدات دولية وكذا الإنابات القاضائية الدولية بصورة مباشرة بدل المرور بالقنوات الدبلوماسية البطيئة التي لا تتماشى وسرعة الجرائم المعلوماتية، إذن نلاحظ أن الدول الغربية قد خطت خطوات فعالة في هذا المجال فماذا عن الدول العربية ؟

من أبرز الجهود العربية في إطار مكافحة جرائم المعلوماتية نجد مثلا:

- القانون العربي الاسترشادي النموذجي لمكافحة الجريمة المعلوماتية المعتمد من قبل جامعة الدول العربية عبر الأمانة العامة لمجلس وزراء العدل العرب وقد اعتمد بالقرار رقم (495 – د – 19-2003/09/08) و قد تضمن القانون 27 مادة موزعة على 04 أبواب، إذ تناول أنواعا للجرائم المعلوماتية دون التعرض لمسألة الاختصاص القضائي

---

[31] وضاح محمود الحمود ونشأت مفضي المجالي ، **جرائم الانترنت** ، دار المنار للنشر والتوزيع ، 2005 ، ص 200 .
[32] جميل عبد الباقي الصغير ، **الجوانب الإجرائية للجرائم المتعلقة بالانترنت** ، دار النهضة العربية ، القاهرة ، 1998 ، ص 79 .



بشكل واضح و لم يشر إلى إخضاع البيانات و المعلومات لطرق إجرائية منسجمة بين الدول العربية، دون التعرض لمفهوم الدليل التقني و حجيته .

– الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية [33] التي وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهم المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21 و تحتوي على 43 مادة موزعة على 05 فصول و هي تهدف إلى تعزيز التعاون القضائي العربي، كما تضمنت هذه الاتفاقية إضافة إلى الشق الموضوعي المتعلق بالتجريم شقا إجرائيا من خلال تفتيش المعلومات وضبط المعلومات المخزنة واعتراض المعلومات، كما تناولت أطر التعاون القانوني والقضائي وتسليم وتبادل المجرمين لكن بشروط عديدة، إضافة إلى تبادل المساعدة القضائية بشرط عدم اعتبار قانون الدولة الطرف المطلوب منها جريمة سياسية أو أنه يشكل انتهاكا لسيادتها أو أمنها أو مصالحها الأساسية.

– إضافة إلى قانون الامارات العربي الاسترشادي لمحاكمة جرائم تقنية المعلومات وما في حكمها المعتمد من قبل وزراء العدل العرب في دورته الـ 19 بالقرار رقم (19/495) بتاريخ 2003/10/08 و اعتمده مجلس وزراء الداخلية العرب في دورته الـــ 21 بالقرار (2004/21/417) يحتوي على 27 مادة تخص العقوبات على الجرائم الاكترونية .

وغيرها من الجهود العربية التي قامت بها هذه الدول في محاولة لتوحيد الجهود العربية لتفعيل قنوات مكافحة الجرائم الإلكترونية، إلا أن معظم النصوص المتفق عليها في إطار هذه المعاهدات والاتفاقيات تبقى في أطر موضوعية تتعلق بالجريمة وعقوبتها، و حتى الحالات التي تضمنت جوانب إجرائية كالاتفاقية العربية لمكافحة الجريمة المعلوماتية رغم ما تضمنته من إجراءات تشكل خطورة نحو تعزيز التعاون الدولي العربي، إلا أنها تواجه صعوبات تتعلق بالاصطدام بمبدأ

[33] الأمانة العامة لجامعة الدول العربية ، **إدارة الشؤون القانونية** ، الشبكة القانونية العربية ، www.arablegalnet.org

السيادة الذي من شأنه أن يعرقل اتخاذ الإجراء متى رأت الدولة أن في الإجراء (التسليم أو غيره) تعارضا مع مبادئها الداخلية، إضافة إلى ضرورة اعتماد الدول العربية هذه الاتفاقية وإدخالها ضمن نظامها القانوني الداخلي حتى توضع فعلا موضع التنفيذ الأمر الذي يجعل موضوع تنفيذ المعاهدة خاضعا لرغبة الدول من عدمه .

إضافة إلى عدم النص على إنشاء شرطة دولية عربية للتنسيق بين أجهزة الشرطة للدول العربية لتسهيل عمليات تسليم المجرمين .

خلاصة:

لنخلص إلى القول أنه رغم ما يواجهه العالم اليوم من خطر محدق فيما يتعلق بالجرائم المعلوماتية إلى أنه لابد من تطوير آليات و طرق مكافحة الجرائم المعلوماتية من الناحية التقنية والقانونية، من خلال تعديل التشريعات الداخلية للدول وخاصة العربية، وكذا تطوير وتحديث آليات التعاون القضائي الدولي وخاصة العربي للحد قدر الإمكان من الجرائم المعلوماتية وتسهيل ملاحقة مرتكبيها بابتكار طرق قانونية و اجرائية جديدة و متطورة تواكب تطور النمط الاجرامي الإلكتروني، لأن المعلوماتية أصبحت تشكل خطرا تزداد آثاره و وحشيته، فمن الحكمة ابتكار آليات ونظم قانونية مستقبلية تضمن قدر الإمكان الوقاية من هذه الجرائم.



قائمة المراجع:

أولا: القوانين والاتفاقيات الدولية

1 -القانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق ل05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها.

2 - قانون جرائم أنظمة المعلومات مؤقت الأردني رقم(30) لعام 2010.

3 - القانون رقم 15/04 المؤرخ في 2004/11/10 المعدل والمتمم لقانون العقوبات الصادر بالأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن القانون المتعلق بالمساس بنظم المعالجة الآلية للمعلومات.

4 - المواد 276 مكرر و مكرر 01 و 02و 03 و 04 في المرسوم السلطاني رقم 2001/72 المنشور بالجريدة الرسمية العمانية رقم 698 بتاريخ 2001/07/01 المعدل لقانون الجزاء العماني الفصل الثاني مكرر مضاف للباب السابع بعنوان جرائم الحاسب الآلي .

5 - اتفاقية بودابست لمكافحة الجرائم المعلوماتية، 2001/11/23، تبناها رؤساء الدول و الحكومات الأعضاء في المجلس الأوروبي.



6 – القانون العربي الاسترشادي النموذجي لمكافحة الجريمة المعلوماتية الأمانة العامة لمجلس وزراء العدل العرب وقد اعتمد بالقرار رقم (495 د – 19-08/09/2003) لجامعة الدول العربية.

7- قانون الامارات العربي الاسترشادي لمحاكمة جرائم تقنية المعلومات (19/495) بتاريخ 10/08/2003 و بالقرار (2004/21/417) .

8- الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لوزراء الداخلية والعدل العرب لجامعة الدول العربية بالقاهرة بتاريخ 21/12/2010 .

ثانيا : الكتب والمؤلفات

1 – الكتب والمؤلفات باللغة العربية

1 – اللبان شريف ، تكنولوجيات الاتصالات : المخاطر و التحديات و التأثيرات الاجتماعية ، الدار المصرية اللبنانية ، القاهرة ، 2000.

2 – أمير فرج يوسف ، **الجرائم المعلوماتية على شبكة الانترنت** ، دار المطبوعات الجامعية ، مصر ، 2009 .

3 – جميل عبد الباقي الصغير ، **الجوانب الإجرائية للجرائم المتعلقة بالانترنت** ، دار النهضة العربية ، القاهرة، 1998.

4 – سامي علي حامد عياد ، **الجريمة المعلوماتية و إجرام الانترنت** ، دار الفكر الجامعية ، الاسكندرية ، 2007.



5 – عبد الفتاح بيومي حجازي، **الدليل الجنائي و التزوير في جرائم الكمبيوتر و الإنترنت**، بهجات للطباعة و التجليد، مصر، 2009.

6 – محمود أحمد عبابنة ، **جرائم الحاسوب و أبعادها الدولية** ، دار الثقافة للنشر و التوزيع ، الأردن، 2005.

7 – نائلة عادلة محمد قورة ، **جرائم الحاسب الآلي الاقتصادية** ، دراسة نظرية و تطبيقية ، منشورات الحلبي الحقوقية ، 2005.

8 – وضاح محمود الحمود ونشأت مفضي المجالي ، **جرائم الانترنت** ، دار المنار للنشر والتوزيع ، 2005 .

2 – الكتب والمؤلفات باللغات الأجنبية

أ – كتب ومؤلفات باللغة الإنجليزية

1 -Merur vender ; computer crimes and other crimes ; against information technologgy in south africa .R.I.D.P . . South Africa ; 1993 .

2 - Adrian Roden ; Computer crimes and the law ; C.L.J . London ; 1991

ب – كتب ومؤلفات باللغة الفرنسية

1 - K trédman.fraude et autres délits d’affairaes commis à l’aide de l’ordinateures éléctroniques.rev.de.pén.crim.Paris.1984.P612.

2 - B.D.Parker. combattre la criminalité informatique . édoro . paris . 1985 .

ثالثا: مقالات قانونية



1 – الرواشدة سامي و الهياجنة أحمد، ((مكافحة الجريمة المعلوماتية كالتجريم و العقاب)) ، المجلة الأردنية في القانون و العلوم السياسية، جامعة مؤتة، الأردن، المجلد الأول، العدد الثالث، 2009.

2 – المرزوقي محمد محمود ، ((الجرائم الحاسب الآلي)) ، المجلة العربية للفقه و القضاء ، صادرة عن الأمانة العامة لجامعة الدول العربية، العدد 28 ، 2003.

3 – هشام محمد فريد رستم ،((الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني)) ، مجلة كلية الشريعة و القانون ، جامعة الإمارات المتحدة ، المجلد الثاني ، الطبعة الثالثة، 2009.

رابعا: أبحاث ومشاركات علمية

1 – رصاع فتيحة ، ((**الحماية الجنائية للمعلومات على شبكة الانترنت**)) ، مذكرة مقدمة لنيل شهادة الماجستير في القانون العام ، جامعة تلمسان ، الجزائر ، 2011 /2012 .

2 – سليم طارق عبد الوهاب ، ((**الجرائم المرتكبة بواسطة الانترنت و سبل مكافحتها**)) ، بحث مقدم إلى الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة ، لمجلس وزراء الداخلية العرب ، تونس ، 07-09-1997.

3 – يونس عرب ، **صور الجرائم المعلوماتية و اتجاهات تبويبها** ، ورقة عمل مقدمة لورشة تطوير التشريعات في مجال مكافحة الجرائم الالكترونية ، هيئة تنظيم الاتصالات ، هيئة تنظيم الاتصالات ، سلطنة عمان ، 2006.

خامسا : المواقع الإلكترونية



1 – الأمانة العامة لجامعة الدول العربية ، **إدارة الشؤون القانونية** ، الشبكة القانونية العربية ،

www.arablegalnet.org

2 – حكومة قطر الإلكترونية ، صفحة المؤتمر :

http//www.moi.gov.qa/UNCCPCJDOha/Arabic /previous – Congrsses . html

